1997

Characterizing the strong two-generators of certain Noetherian domains

Ellen Yvonne Green

CHARACTERIZING THE STRONG TWO-GENERATORS OF CERTAIN NOETHERIAN DOMAINS

A Project

Presented to the

Faculty of

California State University,

San Bernardino

In Partial Fulfillment

of the Requirement for the Degree

Master of Arts

in

Mathematics

---

by

Ellen Yvonne Green

September 1997

CHARACTERIZING THE STRONG TWO-GENERATORS OF CERTAIN NOETHERIAN DOMAINS

A Project

Presented to the

Faculty of

California State University,

San Bernardino

---

by

Ellen Yvonne Green

September 1997

Approved by:

[redacted]

Dr. James Okon, Chair, Mathematics — 9/8/97 Date

[redacted]

Dr. Paul Vicknair

[redacted]

Dr. Davida Fischman

[redacted]

Linda Hintzman

[redacted]

Dr. Terry Hallett, Graduate Coordinator

[redacted]

Dr. Paul Vicknair, Department Chair

ABSTRACT

In this paper we consider the problem of characterizing strong two-generators in certain commutative domains. We will work through the Kerstin Pettersson paper, "Strong n-Generators In Some One-Dimensional Domains," (1994). Specifically, we will work in $K[x^2,x^3]$ where K is any field. We will conclude this paper by verifying the result in Scott Chapman's paper, "Characterizing Strong Two-generators in $K[x^2,x^3]$," (1990). In that paper, Chapman characterized the set of strong two-generators in $K[x^2,x^3]$ as all polynomials which are not contained in the square of the conductor, i.e., not divisible by x^4 over K[x].

TABLE OF CONTENTS

CHAPTER ONE

INTRODUCTION

Let R be a commutative ring with identity. If I is an ideal of R and I can be generated by two elements, then we say that I is two-generated. When all the ideals of R are two-generated then R is said to have the two-generator property. I is said to be strongly two-generated if any nonzero element of I can be chosen as one of the two generators of I. An element r of R is a strong two-generator if r can be chosen as one of the generators of each ideal in which it is contained.

The following work is an adaptation of papers by Chapman [C] and Pettersson [P]. In [C] Chapman characterizes the set of strong two-generators in $K[x^2,x^3]$, for K an arbitrary field. His result was: for f a non-zero element of $K[x^2,x^3]$, if x^2 divides f but x^4 does not, then f is a strong two-generator in $K[x^2,x^3]$.

In [P] Pettersson generalizes Chapman's results to strong two-generators in $K[x^2,x^n]$, where n is any odd integer greater than two. She proved that if p is a nonzero element of $K[x^2,x^n]$ and $m = (x^2,x^n)$, where n is an odd integer greater than two, then p is a strong two-generator if and only if p is not an element of m^2.

The objective of this paper is to reprove Chapman's result [C]. We will do this by using Pettersson's work as a guide. For the most part, Pettersson gives the statement of the propositions and theorems she uses, but leaves the details of the proofs to the reader. In this paper we provide the details of Pettersson's proofs, for the case n = 3.

We assume that all rings are commutative with identity. Since we are concerned with characterizing two-generators, all rings will be finitely generated.

We begin Chapter Two with the definition of a Noetherian ring. We then prove some well-known facts about Noetherian rings. In Proposition 2.7 we decompose ideals into their irreducible components. We look at operations on ideals in Lemma 2.9 (quotients) and Proposition 2.29 (radicals). We conclude Chapter Two with a structure theorem on Artinian rings (a special type of Noetherian ring.) In Chapter Three we will characterize the strong two-generators in $K[x^2,x^3]$.

Let S be the set of all nonzero divisors of an integral domain R. Then $K = S^{-1}R$ is the quotient field of R. A fractional ideal of R is a nonzero R-submodule I of K whose product with some nonzero element of

R is contained in R. A fractional ideal I of R is called invertible if there exists a fractional ideal J of R such that the product of I and J is R.

Pettersson proved in [P], Proposition 3, that an ideal in a one-dimensional Noetherian domain is invertible if and only if it is strongly two-generated. We give a proof of this in Proposition 3.13. In Theorem 3.31 we prove Chapman's result: a nonzero element of R is a strong two-generator in R if and only if x^2 divides it but x^4 does not. To conclude Chapter Three we give two examples. The first is a polynomial in $K[x^2,x^3]$ which is a strong two-generator. The second example is a polynomial in $K[x^2,x^3]$ which is not a strong two-generator.

An appendix follows Chapter Three. It is there that you can find brief statements of the specific theorems and propositions noted in this paper. These are provided to aid the readers of this paper; to help make the references clear.

A great deal of gratitude is offered to my mentor, Dr. James Okon, for without his guidance and expertise, this project would not have been possible.

CHAPTER TWO

NOETHERIAN AND ARTINIAN RINGS

We begin this chapter with basic definitions as we prepare for our work with Noetherian rings.

(2.1) Recall that we assume that all rings are commutative with identity.

(2.2) Definition. An ideal I of a ring R is said to be finitely generated if there exist elements $a_1, a_2, \ldots, a_n$ of I such that every element of I can be written in the form $r_1a_1 + \ldots + r_na_n$, where $r_1, r_2, \ldots, r_n$ are in R. In this case, the a_i are said to be a finite set of generators of I and we write $I = (a_1, \ldots, a_n)$.

(2.3) Definition. A ring R is said to satisfy the ascending chain condition (or to be Noetherian) if for every chain of ideals of R, $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$, there is an integer n such that $I_i = I_n$ for all $i \geq n$.

(2.4) Definition. Let S be a set of ideals. An ideal I, contained in S, is said to be a maximal element of S if for every J in S, $I \subseteq J$ implies that I=J.

Next we show that in a Noetherian ring these three properties are equivalent: that any ideal in the ring is finitely generated, that every nonempty set of ideals contains a maximal element, and that every ascending chain of ideals is eventually stationary.

(2.5) Proposition. For a Noetherian ring R, the following statements are equivalent:

(1) Every ideal in R is finitely generated.

(2) Given a chain of ideals $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$, there exists an n such that $I_n = I_{n+1} = I_{n+2} = \ldots$

(3) Every nonempty set of ideals has a maximal element.

Proof.

(1) implies (2)

Let $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ be a chain of ideals in R and let $I = \bigcup_{i=1}^{\infty} I_i$. First we show that I is an ideal. By definition, I is the union of nonempty sets, thus I is nonempty. If a and b are elements of I, then there exist indices j and k such that a is an element of I_j and b is an element of I_k. Without loss of generality we can assume that $I_j \subseteq I_k$. Then both a and b are elements of I_k. Further, since I_k is an ideal, a+b is an element of I_k. Thus a+b is an element of I. If a belongs to I and r is an element of R, then there exists I_i such that a is an element of I_i. Since I_i is an ideal, ar is an element of $I_i \subseteq I$. Hence I is an ideal of R.

Since every ideal in R is finitely generated and since I is an ideal of R, then there exist $a_1,\ldots,a_k$ such that $I = (a_1,\ldots,a_k)$. For $1 \leq i \leq k$, let n_i be such that a_i is an element of I_{n_i}. Let $n = \max n_i$. Then

a_i is an element of I_n for all $i = 1,\ldots,k$ and $I \subseteq I_n \subseteq I_{n+1} \subseteq \ldots \subseteq I$. Thus $I_n = I_m$ for all $m > n$. Thus we have $I_1 \subseteq I_2 \subseteq \ldots \subseteq I_n = I_{n+1} = \ldots$.

(2) implies (3)

Let A be a set of ideals in R. Suppose that A has no maximal element. Let I_1 be an element of A . Since I_1 is not maximal, there exists an element I_2 in A such that $I_1 \subset I_2$. Since I_2 is not maximal, there exists an element I_3 of A such that $I_1 \subset I_2 \subset I_3$. It follows that because there is not a maximal element in A, we have $I_1 \subset I_2 \subset I_3 \subset \ldots$. But by (2) we know that there exists an n such that $I_n = I_{n+1} = \ldots$, a contradiction. Thus A must have a maximal element.

(3) implies (1)

Let I be an ideal of R and let S be the set of ideals J in R such that $J \subseteq I$ and J is finitely generated. S is nonempty, since $0 \in S$, and S contains a maximal element, say M. Then $M = (m_1, m_2, \ldots, m_n)$ such that $m_i \in I$ for $i = 1,\ldots,n$. If $M \neq I$, let $D = (a, m_1, m_2, \ldots m_n)$ where $a \in I-M$. Then $D \subseteq I$ and $D \in S$. Thus $M \subset D$, a contradiction of the maximality of M, Q.E.D.

We investigate the decomposition of ideals into their irreducible components. Next we give the definition of an irreducible ideal and then in

Proposition 2.7, we show that every ideal is a finite intersection of irreducible ideals.

(2.6) Definition. An ideal I in a ring R is said to be <u>irreducible</u> if $I \neq A \cap B$ where $I \subset A$ and $I \subset B$, for any proper ideals A,B in R. (Equivalently $I = A \cap B$ implies that either I = A or I = B.)

(2.7) Proposition. In a Noetherian ring R every ideal is a finite intersection of irreducible ideals.

Proof. Suppose that I is an ideal of R for which the Proposition is false. Let S denote the set of all such ideals. Then S is non-empty since I is an element of S. By Proposition 2.5 there is a maximal element J in S. Since J is not irreducible, there exist ideals A,B in R such that $J = A \cap B$ where $J \subset A$ and $J \subset B$. Since J is maximal in S, neither A nor B are elements of S. Hence each of A,B is a finite intersection of irreducible ideals and therefore so is J, a contradiction, Q.E.D.

Next we fix our notation for ideal quotients and then show one of their basic properties.

(2.8) Definition. Let A and B be two ideals in a ring R. Their <u>ideal quotient (A:B)</u> is defined to be the set: $\{x \in R \mid xB \subseteq A\}$.

(2.9) Lemma. Let A, B, and C, be ideals in a ring R. If $A \subseteq B$, then $(C:B) \subseteq (C:A)$.

Proof. Suppose that x is an element of (C:B). Then $xB \subseteq C$. Since $A \subseteq B$, $xA \subseteq xB$. Thus $xA \subseteq C$ and x is an element of (C:A), Q.E.D.

In the next lemma we show that if A and B are ideals in a ring R, then their ideal quotient is also an ideal.

(2.10) Lemma. Let A and B be two ideals in a ring R. Then (A:B) is an ideal of R.

Proof. Since $0B = 0 \in A$, $0 \in (A:B)$. Therefore (A:B) is non-empty. Suppose a_1, a_2 are elements of (A:B) and let $b \in B$. Then a_1b is an element of A and a_2b is an element of A. So $(a_1 + a_2)b = a_1b + a_2b$ is an element in A. Also, for each element r of R, we have $(ra_1)b = r(a_1b)$ is an element of A since a_1b is in A and A is an ideal. Thus ra_1 is an element of (A:B) and (A:B) is an ideal, Q.E.D.

(2.11) Remark. We see from Lemmas (2.9) and (2.10) that if A is an ideal of a ring R and b is an element of R, then $(b^n) \subseteq (b^{n-1}) \subseteq \ldots \subseteq (b)$ implies that $(A:(b)) \subseteq (A:(b^2)) \subseteq \ldots$. If R is Noetherian, there exists an $n>0$ such that $(A:(b^n)) = (A:(b^{n+1})) = \ldots$

(2.12) Definition. An ideal A of a Noetherian ring R is said to be <u>primary</u> if for all a and b in R, if ab is in A then either a is in A or b^n is in A for some n. An ideal M in a ring R is said to be a <u>maximal ideal</u>

if $M \neq R$ and for every ideal N of R, $M \subseteq N \subseteq R$ implies that either N = M or N = R.

Primary ideals can be likened to powers of prime numbers in that the primary ideals in the ring of integers are precisely (0) and (p^n) where p is a prime integer. (0) is a primary ideal since the product of two integers is 0 if and only if one of the numbers is itself 0. To see that (p^n) is a primary ideal one needs only to notice that if xy is an element of (p^n) then either x is an element of (p^n) or else p divides y, in which case p^n divides y^n, so $y^n \in (p^n)$.

(2.13) Proposition. In a Noetherian ring R every irreducible ideal is primary.

Proof. Assume that A is an irreducible ideal in R and that A is not primary. Then there exist $a,b \in R$ such that $ab \in A$, $a \notin A$, and $b^n \notin A$ for all n. Choose n as in (2.11) Remark. We now claim that $A = (A:(b^n)) \cap (A + (b^n))$. To see this, let x be an element of $(A:(b^n)) \cap (A + (b^n))$. Then $x = a_1 + b^n r$ for a_1 in A and r in R. Also, $b^n x = b^n(a_1 + b^n r) = b^n a_1 + b^{2n} r \in A$ since $x \in (A:(b^n))$. It follows easily that $b^{2n} r = b^n x - b^n a_1$. Since A is an ideal of R and $b^n x \in A$, $b^n x - b^n a_1 \in A$ which implies that $b^{2n} r \in A$. Thus $r \in (A:(b^{2n})) = (A:(b^n))$ and $b^n r \in A$. So $x = a_1 + b^n r$

is an element of A. Thus $(A:(b^n)) \cap (A + (b^n)) \subseteq A$. For the other containment, if $x \in A$ then $xb^n \in A$, so x is an element of $(A:(b^n))$. Thus $A \subseteq (A:(b^n))$. Furthermore $x = x+0$ and $0 \in (b^n)$, so $x \in (A + (b^n))$ showing that $A \subseteq (A + (b^n))$. Therefore $A \subseteq (A:(b^n)) \cap (A + (b^n))$, proving the claim.

We show now that $A \neq (A + (b^n))$ and $A \neq (A:(b^n))$. $0 \in A$ which implies that $b^n = 0 + b^n \in (A + (b^n))$. But $b^n \notin A$ so $A \neq (A + (b^n))$.

By assumption $ab \in A$ so $a \in (A:(b^n))$. But $a \notin A$ so $A \neq (A:(b^n))$. Thus $A \subset (A:(b^n))$ and $A \subset (A + (b^n))$, a contradiction to the assumption that A is irreducible. Therefore every irreducible ideal is primary, Q.E.D.

(2.14) Proposition. Every ideal of a Noetherian ring is the intersection of primary ideals.

Proof. From Proposition (2.7), for all ideals I in R, $I = A_1 \cap \ldots \cap A_k$ for $i = 1,\ldots,k$ and each A_i is an irreducible ideal in R. By Proposition (2.13), each A_i is primary so I is the intersection of primary ideals, Q.E.D.

(2.15) Definition. Let R be a commutative ring with identity. An element a of R is called a <u>unit</u> of the ring R if $a \cdot b = 1$ for some $b \in R$. The element b is

uniquely determined by a, and is written a^{-1}.

(2.16) Lemma. Let R be a Noetherian ring. Then $a \in R$ is not a unit if and only if $a \in M$ for some maximal ideal M of R.

Proof. Suppose a is not a unit in R. Let S be the set of proper ideals I in R such that $a \in I$. Note: $S \neq \phi$ since $(a) \in S$. By Proposition 2.5, there exists a maximal element, say P, in S. If Q is a proper ideal of R and $P \subset Q \subset R$, then $a \in Q$. Hence $Q \in S$, a contradiction to the assumption that P is a maximal element in S. Thus P is a maximal ideal of R.

Next we show that every element in a maximal ideal is not a unit. Suppose that M is a maximal ideal of R, $m \in M$, and m is a unit. There exists m^{-1} in R such that $1 = m \cdot m^{-1} \in M$. That implies that $1 \in M$, contradicting the supposition that M is a maximal ideal, Q.E.D.

(2.17) Definition. Let I be an ideal of the ring R. The <u>radical of I</u>, denoted rad I, is the set of elements r in R such that $r^n \in I$ for some $n>0$.

(2.18) Definition. An ideal P in a ring R is <u>prime</u> if $P \neq R$ and if $xy \in P$ then either $a \in P$ or $y \in P$.

(2.19) Lemma. Let A and B be ideals in a ring R. If $A \subseteq B$ then rad $A \subseteq$ rad B.

Proof. Assume $A \subseteq B$. If $r \in \operatorname{rad} A$ then there exists $n > 0$ such that $r^n \in A \subseteq B$. Thus $r \in \operatorname{rad} B$, Q.E.D.

(2.20) Lemma. If $I_1, \ldots, I_n$ are ideals in a ring R then $\operatorname{rad} (\bigcap_{i=1}^{n} I_i) = \bigcap_{i=1}^{n} (\operatorname{rad} I_i)$.

Proof. If $r \in \operatorname{rad} (\bigcap_{i=1}^{n} I_i)$ then there exists $m > 0$ such that $r^m \in \bigcap_{i=1}^{n} I_i$. That implies for $i = 1, \ldots, n$, $r^m \in I_i$, $r \in \operatorname{rad} I_i$, and $r \in \bigcap_{i=1}^{n} (\operatorname{rad} I_i)$.

To see the other inclusion suppose that $r \in \bigcap_{i=1}^{n} (\operatorname{rad} I_i)$. Then there exist $m_1, m_2, \ldots, m_n > 0$ such that $r^{m_i} \in I_i$ for each i. If $m = m_1 m_2 \ldots m_n$, then $r^m \in \bigcap_{i=1}^{n} I_i$. Thus $r \in \operatorname{rad} (\bigcap_{i=1}^{n} I_i)$, Q.E.D.

(2.21) Lemma. Let $I_1, I_2, \ldots, I_n$ be ideals in a ring R and let P be a prime ideal containing $\bigcap_{i=1}^{n} I_i$. Then $P \supseteq I_i$ for some i.

Proof. Suppose $P \not\supseteq I_i$ for all i. Then there exist $x_i \in I_i$ such that $x_i \notin P$, $1 \leq i \leq n$. Then $x_1 x_2 \ldots x_n \in \bigcap_{i=1}^{n} I_i$ but $x_1 x_2 \ldots x_n \notin P$. Thus $P \not\supseteq \bigcap_{i=1}^{n} I_i$, Q.E.D.

(2.22) Remark. It can be shown that the radical of an ideal I is the intersection of all prime ideals which contain I [A-M, Proposition 1.14, page 9].

(2.23) Definition. A nonzero element a in a ring R is said to a <u>zero divisor</u> if there exists $b \in R$ such that $b \neq 0$ and $ab = ba = 0$.

(2.24) Definition. A commutative ring R with identity $1 \neq 0$ and no zero divisors is called an integral domain.

(2.25) Remark. Every integral domain has at least two elements: 0 and 1.

(2.26) Remark. Every field K is an integral domain since $ab = 0$ and $a \neq 0$ imply that $b = 1b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}(0) = 0$.

(2.27) Example. (0) in any integral domain is a prime ideal since for $ab = 0$ either $a = 0$ or $b = 0$.

(2.28) Example. If p is a prime integer, then the ideal (p) in Z is prime. To see this assume that $ab \in (p)$. Then p ab so either p a or p b which implies that $a \in (p)$ or $b \in (p)$.

(2.29) Proposition. If I is a primary ideal in a commutative ring R, then rad I is a prime ideal.

Proof. Assume that $ab \in$ rad I and that $a \notin$ rad I. Then $a^n \notin I$ for all $n>0$. Since $(ab)^n \in I$ for some $n>0$, $a^n b^n \in I$. By assumption $a^n \notin I$ and I is primary, so there is an integer $m>0$ such that $(b^n)^m \in I$. Then $b^{nm} \in I$ so $b \in$ rad I. Therefore rad I is prime, Q.E.D.

(2.30) Definition. If I is a primary ideal in a commutative ring R, then J = rad I is called the associated prime ideal of I.

(2.31) Definition. Let R be a Noetherian ring and

I be an ideal in R. An ideal I has a primary decomposition if $I = Q_1 \cap Q_2 \cap \ldots \cap Q_n$ and each Q_i is a primary ideal of R. If $I = Q_1 \cap \ldots \cap Q_n$ is a primary decomposition of I then the set of <u>associated prime ideals of I</u>, denoted Ass(R/I), is precisely $\{P_1, P_2, \ldots, P_n\}$ where each $P_i = \text{rad } Q_i$. It can be shown that the P_i are independent of the particular decomposition of I [1].

(2.32) Example. (cf. [H, page 380]) If p is a prime in Z, then (p) is the associated prime ideal of (p^2), (p^3), ... It follows easily from Definition 2.30, that since (p^n) is a primary ideal, rad $(p^n) = (p)$ is the associated prime ideal of (p^n).

(2.33) Definition. A chain of prime ideals $P_0 \supset P_1 \supset P_2 \supset \ldots \supset P_n$ in a ring R is said to have length n. The <u>dimension</u> of R is said to be the maximum length of all chains of prime ideals in R: it is an integer ≥ 0, or positive infinity (assuming $R \neq 0$).

(2.34) Definition. A ring R is said to satisfy the <u>descending chain condition</u> (or to be <u>Artinian</u>) if for every chain of ideals $I_1 \supseteq I_2 \supseteq \ldots$ of R there is an integer n such that $I_i = I_n$ for all $i \geq n$.

(2.35) Remark. It can be shown that a 0-dimensional Noetherian ring is an Artinian ring, and vice-versa

[2]. The proof relies on the fact that every prime ideal in an Artinian ring is maximal and that the intersection of these maximal ideals is 0.

(2.36) Example. A field R is Artinian since the only ideals are 0 and R. It follows from the next proposition that the ring of integers mod n, $n \neq 0$, is Artinian (in part ii we show that the dimension of R/(a) is 0). We will use $\bar{I}$ to denote the image in R/I of the ideal I in R which contains a.

(2.37) Proposition. Let R be a one-dimensional Noetherian integral domain and let a be a nonzero element of R. Then:

(i) Each prime ideal in R/(a) is of the form $\bar{M}$, where M is a maximal ideal of R containing a.

(ii) R/(a) is Artinian.

Proof.

(i) Let $(a) = Q_1 \cap Q_2 \cap \ldots \cap Q_n$ be a primary decomposition of (a). Then rad $Q_i \supseteq (a) \supset (0)$. We have that (0) is prime by Example 2.27. From Proposition 2.29, rad Q_i are prime since Q_i are primary. There are exactly two prime ideals in any length one chain of prime ideals, so every non-zero prime ideal in a one-dimensional domain is maximal. Thus, rad Q_i are

maximal ideals in R. Let M_i = rad Q_i for $1 < i < n$. Let f be the ring homomorphism $f: R \longrightarrow R/(a)$ defined by $f(y) = y + (a) = \bar{y}$.

We show now that if Q is a prime ideal in R/(a) then $f^{-1}(Q)$ is a prime ideal in R containing a. Suppose that $xy \in f^{-1}(Q)$. Then $f(x)f(y) \in Q$ which implies that either $f(x) \in Q$ or $f(y) \in Q$. Thus $x \in f^{-1}(Q)$ or $y \in f^{-1}(Q)$ so $f^{-1}(Q)$ is a prime ideal in R containing a. Let $P = f^{-1}(Q)$. Then $(a) \subseteq P$, so $P \supseteq \bigcap_{i=1}^{n} Q_i$. From Lemma 2.19 it follows that rad $P \supseteq$ rad $(\bigcap_{i=1}^{n} Q_i)$.

We show now that if P is prime then rad P = P. Choose $x \in$ rad P. Then $x^n \in P$ for some $n > 0$ which implies that $x \in P$. To see the other containment, suppose $x \in P$. Clearly $x^n \in P$ so $x \in$ rad P.

So $P \supseteq$ rad $(\bigcap_{i=1}^{n} Q_i) = \bigcap_{i=1}^{n}$ rad $Q_i = \bigcap_{i=1}^{n} M_i$. Thus $P \supseteq \bigcap_{i=1}^{n} M_i$. From Lemma 2.21 we have that $P \supseteq M_i$ for some i. Since rad Q_i is maximal, P = rad Q_i. Also, $f^{-1}(Q) = P = M_i$ so $Q = f(M_i) = \bar{M}_i$. Thus each prime ideal in R/(a) is of the form $\bar{M}$ for some maximal ideal M in R containing a.

(ii) Since R is a Noetherian ring, R/(a) is a Noetherian ring [3]. Thus, it is enough to show that dim(R/(a)) = 0. We do this by showing that every prime ideal in R/(a) is maximal.

Let f and Q be the same as in part (i) above. Suppose that Q is not a maximal ideal. Then there exists a maximal ideal $N \subset R/(a)$ such that $Q \subset N$. Let $y \in N-Q$ and let $u \in f^{-1}(y)$. By part (i), $f^{-1}(Q)$ is a prime ideal of R. Since R is a one-dimensional ring, $f^{-1}(Q)$ is a maximal ideal of R, so $(1) = (u, f^{-1}(Q))$. There exists $r \in R$ and $t \in f^{-1}(Q)$ such that $\overline{1} = ru + t$. Then $1 = f(1)$ $= f(ru + t) = f(ru) + f(t) = f(r)f(u) + f(t)$. Since $f(r) \in R/(a)$ and $f(u) \in N$, then $f(r)f(u) \in N$. Also, $f(t) \in Q \subset N$ so $\overline{1} \in N$, a contradiction to the maximality of N. Thus every prime ideal in R/(a) is a maximal ideal. Hence R/(a) is a 0-dimensional Noetherian integral domain, Q.E.D.

Next we give the statement of the Chinese Remainder Theorem. A proof can be found in [H, page 131].

(2.38) The Chinese Remainder Theorem. Let $A_1,\ldots,A_n$ be ideals in a ring R such that $A_i + A_j = R$ for all $i \neq j$. If $b_1,\ldots,b_n$ are elements of R then there exists $b \in R$ such that b is congruent to b_i (mod A_i) for $i = 1,\ldots,n$.

(2.39) Definition. [c.f. A-M, page 7] Let $R_1,\ldots,R_n$ be rings. Their <u>direct product</u> $R = \prod_{i=1}^{n} R_i$ is the set of all sequences $x = (x_1,\ldots,x_n)$ with $x_i \in R_i$, $1 \leq i \leq n$, and componentwise addition and multiplication. Note:

R is a commutative ring with identity element $(1,\ldots,1)$. We call the mappings $p_i: R \longrightarrow R_i$ defined by $p_i(x) = x_i$ the canonical <u>projections</u> of the product onto its i^{th} component.

(2.40) Definition. Let R be a ring. Let S be a subset of R such that $0 \notin S$, $1 \in S$ and if $x,y \in S$ then $xy \in S$. Define an equivalence relation on the set RxS by

$$(r,s) \sim (r',s') \Leftrightarrow s_1(rs' - r's) = 0 \text{ for some } s_1 \in S.$$

One can easily verify that $\sim$ is reflexive, symmetric, and transitive. The equivalence class $(r,s) \in RxS$ will be denoted r/s. The set of all equivalence classes will be denoted by $S^{-1}R$. We put a ring structure on $S^{-1}R$ by defining addition and multiplication in the same way as for fractions:

$$(r/s) + (r'/s') = (rs' + r's)/ss',$$

$$(r/s)(r'/s') = rr'/ss'.$$

We note that if R is an integral domain, then $S^{-1}R$ is an integral domain [4].

(2.41) Definition. If R is a ring, P a prime ideal of R, and S = R-P, then $S^{-1}R$ is called the <u>localization of R at P</u> and is denoted R_P. If I is an ideal in R, then the ideal $S^{-1}I = \{a/s \text{ such that } a \in I;\ s \in S\}$ in R_P is denoted I_P. It can be proved that $S^{-1}I$ is an ideal of $S^{-1}R$ [5].

We note that $R_P = \{r/s \text{ such that } r \in R \text{ and } s \in R-P\}$.

We now prove a structure theorem for Artinian rings.

(2.42) Theorem. Let R be an Artinian ring. Then

(i) R has only a finite number of maximal ideals.

(ii) If $M_1,\ldots,M_n$ are the maximal ideals of R then there is an isomorphism of rings $R \cong \prod_{i=1}^{n} R_{M_i}$.

Proof. (i) Let $(0) = Q_1 \cap Q_2 \cap \ldots \cap Q_n$ be a primary decomposition of (0) in R. We will show that all the maximal ideals in R are of the form rad Q_i for some i. Let M_i = rad Q_i for $i = 1,\ldots,n$ and let M be a maximal ideal of R. Then $0 \in M$ since M is an ideal. So $M \supseteq (0) = \bigcap_{i=1}^{n} Q_i$ and we have that $M = \text{rad } M \supseteq \bigcap_{i=1}^{n} \text{rad } Q_i = \bigcap_{i=1}^{n} M_i$. Thus $M \supseteq \bigcap_{i=1}^{n} M_i$. Since every maximal ideal in R is prime, we have that $M \supseteq M_i$ for some i. Each M_i is maximal so $M = M_i$ for some i.

(ii) Define a mapping $\phi: R \to \prod_{i=1}^{n} R/Q_i$ by $\phi(r) = (r + Q_1,\ldots,r + Q_n)$. We verify that ϕ is a homomorphism. Let $r_1,r_2 \in R$. Then $\phi(r_1 + r_2) = (r_1+r_2 + Q_1,\ldots,r_1+r_2 + Q_n) = (r_1 + Q_1,\ldots,r_1 + Q_n) + (r_2 + Q_2,\ldots,r_2 + Q_n) = \phi(r_1) + \phi(r_2)$. Also, $\phi(r_1r_2) = (r_1r_2 + Q_1,\ldots,r_1r_2 + Q_n) = (r_1 + Q_1,\ldots,r_1 + Q_n)(r_2 + Q_1,\ldots,r_2 + Q_n) = \phi(r_1)\phi(r_2)$. To see that ϕ is onto we use Chinese Remainder Theorem. We must show that $Q_i + Q_j = R$. Since Q_i and Q_j are primary ideals of R, rad Q_i and

rad Q_j are prime ideals in R. Recall that R is an Artinian ring so rad Q_i and rad Q_j are maximal ideals of R. Thus R = rad Q_i + rad Q_j. Since $Q_i, Q_j \subseteq Q_i+Q_j$, rad Q_i, rad $Q_j \subseteq$ rad (Q_i+Q_j) by Lemma 2.19. So R = rad Q_i + rad $Q_j \subseteq$ rad $(Q_i+Q_j) \subseteq R$, thus rad (Q_i+Q_j) = R. Therefore, $1 \in$ rad (Q_i+Q_j), $1 \in Q_i+Q_j$, and Q_i+Q_j = R. By the Chinese Remainder Theorem, if $b_i \in R$ then there exists $b \in R$ such that $b \equiv b_i \bmod Q_i$ for $i = 1,\ldots,n$, and ϕ is onto.

Now $r \in \ker \phi$ if and only if $\overline{r} = \overline{0}$ in R/Q_i for all i, if and only if r is an element of Q_i for all i, if and only if $r \in \bigcap_{i=1}^{n} Q_i = (0)$, so ϕ is one-to-one.

Now we show that $R/Q_i \cong {}^{R}M_i$ for all i. Without loss of generality let i = 1. Define a ring homomorphism $f: R \rightarrow {}^{R}M_1$ by $f(x) = x/1$. It is easily seen that f(x) + f(y) = f(x + y) and f(xy) = f(x)f(y), so ϕ is a homomorphism. Suppose $x \in \ker f$. Then $f(x) = x/1 = 0/s$ for some $s \in R-M_1$ which implies that $s_1(xs - 0 \cdot 1) = s_1(xs) = (s_1s)x = 0$. Both s_1 and s are elements of $R-M_1$ so $s_1s \in R-M_1$. Since M_1 = rad Q_1, $(s_1s)^m \notin Q_1$ for all m. Further, $x \in Q_1$ since Q_1 is a primary ideal. So $\ker f \in Q_1$. For the opposite inclusion, let x be a nonzero element of Q_1. Since $x \neq 0$, there exists a k such that x is an element of $Q_1 \cap Q_2 \cap \ldots \cap Q_k$ but

$x \in Q_{k+1}, \ldots, Q_n$. Further, $(Q_i:x) = R$ for $i = 1,\ldots,k$ and rad $(Q_i:x) = M_i$ for $i = k+1,\ldots,n$ [6]. Thus $(0:x) = ((\bigcap_{i=1}^{n} Q_i):x) = \bigcap_{i=1}^{n}(Q_i:x) = \bigcap_{i=k+1}^{n}(Q_i:x)$. Suppose $(0:x) \subseteq M_1$. Then $M_1 = \text{rad } M_1 \subseteq \text{rad } (0:x) = \text{rad } (\bigcap_{i=1}^{n}(Q_i:x)) = \bigcap_{i=1}^{n}\text{rad } (Q_i:x) = \bigcap_{i=1}^{n} M_i$. Thus $M_{k+1} \cap \cdots \cap M_n \subseteq M_1$, a contradiction. So $(0:x) \subseteq M_1$ and there exists $s \in R-M_1$ such that $sx = 0$. Since $s \in R-M$ and $0 \in M$, $s \neq 0$. By definition $x \neq 0$ and R has no zero divisors, so $x/1 = 0/s$. Thus $x \in \ker f$ and $\ker f = Q$. Next we show that f is onto. Let $x/s \in {}^{R}M_1$, $s \notin M_1$. Note: $s \notin \bigcup_{i=1}^{n} M_i$ implies s is a unit (Lemma 2.16). So there exists $s^{-1} \in R - \bigcup_{i=1}^{n} M_i$ such that $ss^{-1} = 1$. Thus $f(xs^{-1}) = (xs^{-1})/1 = (xs^{-1}s)/1s = x/s$. Suppose $s \in M_2-M_1$. Since $1 \in R$, $s = s1 \in sR \notin M_1$, so $sR + Q_1 \notin M_1$. Suppose $Q_1 \subseteq M_i$, $i=1,\ldots,n$. Since R is an Artinian ring, for all i, rad $Q_1 = M_i$, implying $M_1 = M_i$, a contradiction. Thus $sR + Q_1 \subseteq M_i$, for any i, and $sR + Q_1 = R$ so $1 \in sR + Q_1$. Then $1 = rs + b$ for $r \in R$ and $b \in Q_1$. Thus $x = xrs + xb$ and $f(x) = f(xrs + xb) = f(xrs) + f(xb)$. Since $xb \in \ker f$, $f(xb) = 0$. Thus $x/1 = xrs/1$, $x/s = xr/1 = f(xr)$, and f is onto. We show that f is one-to-one. Let $r_1, r_2 \in R$. Then $f(r_1) = f(r_2)$ if and only if $r_1/1 = r_2/1$ if and only if $r_1 = r_2$. Thus f is an isomorphism and $\prod_{i=1}^{n} R/Q_i = \prod_{i=1}^{n} R_M$, so $R \cong \prod_{i=1}^{n} R_M$, Q.E.D.

CHAPTER THREE

CHARACTERIZING STRONG TWO-GENERATORS

In this chapter we will prove some of the theorems of sections two and three of Kerstin Pettersson's paper, "Strong n-Generators In Some One-Dimensional Domains." Specifically, we prove those theorems which are needed to characterize strong two-generators in $K[x^2,x^3]$ where K is an arbitrary field. In some cases, we needed to prove some basic results not explicitly proven in [P].

(3.1) Definition. Let $\mathfrak{X}$ be a subset of a ring R. Let $\{A_i \mid i \in I, I \text{ an index set}\}$ be the family of all ideals in R which contain $\mathfrak{X}$. Then $\cap A_i$ is called the ideal generated by $\mathfrak{X}$, denoted $(\mathfrak{X})$. The elements of $\mathfrak{X}$ are called generators of the ideal $(\mathfrak{X})$.

A ring element which can be chosen as one of the generators of each ideal in which it is contained is called a strong generator.

(3.2) Definition. If I is an ideal of a commutative ring R and I can be generated by two elements of R, then I is two-generated. A ring R has the two-generator property if each ideal of R is two-generated.

(3.3) Definition. A nonzero element of a commutative ring R is a strong two-generator if it can be chosen as one of two generators of each ideal in which it is contained.

We show now that an element is a strong

two-generator in a direct product of rings if and only if it is a strong two-generator in each factor.

(3.4) Proposition. Let R, R_1, R_2, ..., R_n be rings such that $R \cong \prod_{i=1}^{n} R_i$ and R has the two-generator property. Let $\phi: R \longrightarrow \prod_{i=1}^{n} R_i$ denote the isomorphism and ϕ_j denote the projection maps: $\phi_j: \prod_{i=1}^{n} R_i \longrightarrow R_j$. Then $f \in R$ is a strong two-generator in R if and only if $\phi_i(f)$ is a strong two-generator in R_i for all $i = 1,\ldots,n$.

Proof. Note that since $R \cong \prod_{i=1}^{n} R_i$, we'll consider R and $\prod_{i=1}^{n} R_i$ equal for simplicity of notation. Assume that f is a strong two-generator in R. Let I_j be an ideal in R_j such that $\phi_j(f) \in I_j$. Then $f \in \phi_j^{-1}(I_j)$. Since f is a strong two-generator in R, then f can be chosen as one of the two generators of all ideals in R which contain f. We show that $\phi_j^{-1}(I_j)$ is an ideal. Let $f_1, f_2 \in \phi_j^{-1}(I_j)$. Then $\phi_j(f_1)$, $\phi_j(f_2) \in I_j$. Since I_j is an ideal in R_j, $\phi_j(f_1)-\phi_j(f_2) \in I_j$. Further, ϕ_j is a ring homomorphism, so $\phi_j(f_i)-\phi_j(f_2) = \phi_j(f_1-f_2)$ which puts f_1-f_2 in $\phi_j^{-1}(I_j)$. Let $r \in R$. Then $\phi_j(r) \in R_j$. Since I_j is an ideal in R_j, $\phi_j(r)\phi_j(f_1) \in I_j$. Further, ϕ_j is a ring homomorphism, so $\phi_j(r)\phi_j(f_1) = \phi_j(rf_1)$ putting rf_1 in $\phi_j^{-1}(I_j)$.
So there exists $g \in R$ such that $\phi_j^{-1}(I_j) = (f,g)$.
Applying ϕ_j to both sides, $I_j = \phi_j(f,g)$. But

$\phi_j(f,g) = (\phi_j(f),\phi_j(g))$ so $\phi_j(f)$ is a strong two-generator. For the converse, let I be an indeal of R, let $f = (\phi_1(f),\ldots,\phi_n(f)) \in I$, and let $\phi_j(I) = I_j$. Assume that $\phi_j(f)$ is a strong two-generator in R_j for all j. Since $\phi_j(f) \in I_j$ there exists $g_j \in I_j$ such that $I_j = (\phi_j(f),g_j)$. Let $g \in R$ such that $g = (g_1,\ldots,g_n)$. We claim that $I = (f,g)$. Assume that $x = (x_1,\ldots,x_n) \in I$. Since $\phi_j(f)$ and g_j are generators of I_j for $1 \leq j \leq n$, $x_j = a_j\phi_j(f) + b_jg_j$ for $a_j,b_j \in R_j$. Suppose $a = (a_1,\ldots,a_n)$ and $b = (b_1,\ldots,b_n)$. Then $x = (a_1\phi_1(f) + b_1g_1, \ldots, a_n\phi_n(f) + b_ng_n) = (a_1\phi_1(f),\ldots,a_n\phi_n(f)) + (b_1g_1, \ldots,b_ng_n) = (a_1,\ldots,a_n)(\phi_1(f),\ldots,\phi_n(f)) + (b_1,\ldots,b_n)(g_1,\ldots,g_n) = af + bg$. Thus $I = (f,g)$, Q.E.D.

(3.5) Definition. Let R be a commutative ring. An <u>R-module</u> is an additive abelian group A together with a function $f: R\times A \longrightarrow A$ such that, if we write ra for f(r,a), the following axioms are satisfied for $a,b \in A$ and $r,s \in R$: (i) $r(a + b) = ra + rb$,

(ii) $(r + s)a = ra + sa$,

(iii) $r(sa) = (rs)a$,

(iv) $1a = a$ whenever R has identity.

A <u>submodule</u> A' of A is an additive subgroup of A which is closed under multiplication by elements of R.

(3.6) Definition. Let S be the set of all nonzero elements in an integral domain R. Then $K = S^{-1}R$ is the quotient field of R. An R-submodule I of K is a fractional ideal of R if $xI \subseteq R$ for some $x \neq 0$ in R. Thus the ideals of R are fractional ideals (take x = 1), and in that case we call I an ordinary ideal of R.

(3.7) Definition. Let R be an integral domain with quotient field K. Let I be a fractional ideal of K. The fractional ideal I^{-1} (the inverse of I) is the set of all x in K such that $xI \subseteq R$. I is called invertible if $II^{-1} = R$. If I is an ordinary ideal of R then $R \subset I^{-1}$. If I is a fractional ideal then $I^{-1} \subset R$.

We show now that localization at maximal ideals preserves invertibility of ideals.

(3.8) Lemma. Let R be an integral domain and let I, M be ideals in R such that M is maximal in R. If I is invertible then $I_M = \{ i/s \mid i \in I , s \in R-M \}$ is invertible for all M.

Proof. Since $II^{-1} = R$, there exist $a_i \in I$, $b_i \in I^{-1}$ such that $1 = \sum_{i=1}^{n} a_i b_i \in II^{-1}$. Also $I \subseteq I_M$ since for all a in I, $a/1 \in I_M$.

To see that $I^{-1} \subseteq I_M^{-1}$, let x be an element of I^{-1}. Then $xI \subseteq R$. Let $\alpha/t \in I_M$, $\alpha \in I$, $t \in R-M$. Then $x(\alpha/t)$

$= x\alpha/t \in R_M$ since $x\alpha \in R$. Thus $xI_M \subseteq R_M$ and $x \in I_M^{-1}$. Now $1 \in I_M I_M^{-1}$ so $R_M = I_M I_M^{-1}$, Q.E.D.

(3.9) Definition. Let I be an ideal of a ring R. I is called a <u>principal ideal</u> if $I = (a) = \{xa \mid x \in R\}$ for some $a \in I$.

(3.10) Theorem. Let R be an integral domain and let I be a fractional ideal of R. If I is invertible then I is a finitely generated R-module.

Proof. If I is invertible then $II^{-1} = R$. Thus there exist $a_i \in I$ and $b_i \in I^{-1}$ such that $1 = \sum_{i=1}^{n} a_i b_i$. We will show that the a_i's generate I. If $x \in I$ then $x = 1x = x\sum_{i=1}^{n} a_i b_i = \sum_{i=1}^{n} (xb_i)a_i$. All of the elements xb_i lie in R since $x \in I$ and $b_i \in I^{-1}$. Thus $I = (a_1, \ldots, a_n)$ proving the claim, Q.E.D.

(3.11) Proposition. Let R be a Noetherian integral domain and let I be a fractional ideal of R. Then I is invertible if and only if I_M is a principal ideal for each maximal ideal M of R.

Proof. Assume that I is invertible. Then I_M is invertible (Lemma 3.8). Since I is invertible, I is finitely generated (Theorem 3.10). There exist $a_i \in I_M$ and $b_i \in I_M^{-1}$ such that $\sum_{i=1}^{n} a_i b_i = 1$. Since $1 \notin MR_M$, one of the $a_i b_i$, say $a_1 b_1$, is not an element of MR_M. We will show that $I_M = (a_1)$.

Since $a_1b_1 \in MR_M$ and MR_M is the only maximal ideal of R_M, a_1b_1 is a unit in R_M by Lemma 2.16. Let $\alpha \in I_M$. Then $\alpha = (\alpha a_1b_1)/(a_1b_1) = (a_1 \alpha b_1)/(a_1b_1)$ $= (a_1 \alpha 1)/((a_1b_1)b_1)$. Now $1/((a_1b_1)b_1) \in R_M I_M^{-1} = I_M^{-1}$ and $\alpha \in I_M$ so $\alpha \in a_1R_M$. Thus $\alpha \in (a_1)$. So $I_M \subseteq (a_1)$ and the opposite inclusion holds since $a_1 \in I_M$. Thus $I_M = (a_1)$.

Now assume that I_N is a principal ideal for each maximal ideal N of R. Suppose that $II^{-1} \subseteq M \subset R$ for some maximal ideal M of R. Since I is finitely generated, $I = (a_1,\ldots,a_n)$ with $a_i \in I$. Then $I_M = (a)$ for some $a \in I$. If $a_i \in (a)$ then $a_i = (r_i/s_i)a$ for some $r_i \in R$ and $s_i \in R-M$. So $(s_i/a)a_i = r_i \in R$. Let $s = s_1s_2\ldots s_n$. Then $(s/a)I \subseteq R$. Thus $s/a \in I^{-1}$ and $s = (s/a)a \in II^{-1} \subseteq M$. Then $s \in M$, a contradiction, Q.E.D.

(3.12) Definition. Let R be a ring with identity and let I be a proper ideal of R which can be generated by two elements. I is said to be <u>strongly two-generated</u> if any nonzero element of I can be chosen as one of two generators of I.

Now we show that there is a connection between the property of being strongly two-generated and the invertibility of an ideal.

(3.13) Proposition. Let R be a Noetherian one-dimensional integral domain. Let I be a fractional ideal of R. Then I is invertible if and only if I is strongly two-generated.

Proof. Let I be a fractional ideal of R with quotient field K. By Theorem 3.10, I is finitely generated as an R-module. Let I be generated by $c_1,\ldots,c_n \in K$ such that for each i, $c_i = r_i/s_i$ with $0 \neq s_i$, $r_i \in R$. Let $s = s_1 s_2 \cdots s_n$. Then $I' = sI$ is an ideal of R and $s^{-1}I' = I$.

We will now show that $I'(I')^{-1} = R$ if and only if $II^{-1} = R$. Suppose that $I'(I')^{-1} = R$. Then there exist $a_i \in I'$ and $b_i \in (I')^{-1}$ such that $1 = \sum_{i=1}^{n} a_i b_i$. Since $I' = sI$, there exist $d_i \in I$ such that $sd_i = a_i$, for all i. So $1 = \sum_{i=1}^{n} (sd_i)b_i = \sum_{i=1}^{n} d_i(sb_i)$. Now $b_i I'$ is a subset of R which implies that $b_i(sI) = (sb_i)I \subseteq R$, therefore $sb_i \in I^{-1}$. Thus $II^{-1} = R$.

Suppose that $II^{-1} = R$ and let s be as above. Then there exist $a_i \in I$, $b_i \in I^{-1}$ such that $1 = \sum_{i=1}^{n} a_i b_i = \sum_{i=1}^{n} sa_i(b_i/s)$. Since $a_i \in I$ we have that $sa_i \in I'$. Since $b_i \in I^{-1}$, $(b_i/s)I' = (b_i/s)sI = b_i I \subseteq R$ so $b_i/s \in (I')^{-1}$. Thus $I'(I')^{-1} = R$. Hence it is enough to prove the statement of Proposition 3.13 for I an ideal of R.

Assume that I is an invertible ideal of R and that a is a nonzero element of I. By Proposition 3.11, for I invertible, I_M is a principal ideal for M a maximal ideal of R. I is an ideal implies that I/(a) is an ideal. Since $(I/(a))_M \cong I_M/(a)_M$, if I_M is principal then $(I/(a))_M$ is principal [7]. So $I/(a) \cong \prod_{i=1}^{n} (I/(a))_M$ by Theorem 2.37 and Theorem 2.42 and I/(a) is principal. Therefore I is strongly two-generated.

To see the opposite implication assume that I is a strongly two-generated ideal of R and that M is a maximal ideal of R. If $I \nsubseteq M$ then $I_M = R_M$.
(Note: There exists an element a in I-M and a/a is an element of I_M since a is an element of R-M).
Suppose that $I \subseteq M$. Let $am \in IM$ for some $a \in I$ and $m \in M$. Since I is strongly two-generated I = (am,b) for some $b \in I$. Since $a \in I$, $a = r_1ma + r_2b$, for some $r_1, r_2 \in R$. This implies that $a - r_1ma = r_2b$. Thus $a(1 - r_1m) \in bR$. Since $1 - r_1m \in R-M$, $1 - r_1m$ is a unit in R_M. Thus $a \in bR_M$ and hence $I_M = bR_M$. By Proposition 3.11, since I_M is principal, I is invertible, Q.E.D.

(3.14) Definition. [K, p.67] A ring is <u>local</u> if it is Noetherian and has exactly one maximal ideal.
Note: Since every proper ideal in a ring with identity is contained in some maximal ideal, the unique maximal

ideal of a local ring must contain all proper ideals of R.

(3.15) Definition. A principal ideal ring, PIR, is a ring in which every ideal is principal. A PIR which is an integral domain is a principal ideal domain, PID.

(3.16) Example. Z_M, $F_1 \times F_2$ such that F_1 and F_2 are fields, and any homomorphic image of a PIR are examples of a PIR.

(3.17) Example. Z and K[x] such that K is a field, are examples of a PID.

Next we state Theorem 4 of Kirsten Pettersson's paper, "Strong n-Generators In Some One-Dimensional Domains." We will not prove the theorem here but a proof can be found in Pettersson's paper.

We have seen a connection between the property of being strongly two-generated and invertibility of an ideal (Proposition 3.13.) We would like to know if there exists a connection between strong two-generators and invertibility of ideals. Among other results, Theorem 3.18 states that a nonzero element in a two-generated domain D is a strong two-generator if and only if it is not contained in the square of any non-invertible maximal ideal M of D.

(3.18) Theorem. (cf. [Pettersson, Theorem 4]) Let D be a two-generated domain and a be a nonzero element of D. Then the following are equivalent:

(1) $a \notin M^2$ for each non-invertible maximal ideal M of D.

(2) D/(a) is a principal ideal ring (PIR) in all its localizations at maximal ideals.

(3) D/(a) is a PIR.

(4) a is a strong two-generator in D.

(3.19) Definition. If R is a ring with identity and f(x) is an element of R[x] with leading coefficient 1 then f(x) is said to be a monic polynomial.

(3.20) Definition. Let S be a ring and R be a nonempty subset of S that is closed under the operations of addition and multiplication in R. If R is also a ring under those same operations then R is a subring of S.

(3.21) Definition. Let S be a ring with identity 1_S and let R be a subring of S containing 1_S. Then S is said to be an extension ring of R.

(3.22) Definition. Let S be an extension ring of R and let $s \in S$. If there exists a monic polynomial $f(x) \in R[x]$ such that s is a root of f(x), i.e. f(s) = 0, then s is said to be integral over R. We say that R' is the integral closure of R in S whenever R' is

The set of all elements of S that are integral over R. If S is not explicitly mentioned we will assume that S is the quotient field of R. If S = R' then S is said to be an integral extension of R.

(3.23) Definition. Let R be a Noetherian integral domain with integral closure S. The conductor C of R in S is defined as $C = [R : S] = \{y \in R$ such that $yS \subseteq R\}$.

(3.24) Proposition. Let R be a Noetherian integral domain with integral closure S. Let C be the conductor of R in S. Then C is an ideal of both R and S.

Proof. Since $0S = 0 \in R$, $0 \in C$, and C is nonempty. Let $a \in C$ and let $s', s'' \in S$. Then $(s'a)s'' = a(s's'') \in aS \subseteq R$ since $a \in C$, so C is an ideal of S. Since C is an ideal of S and $R \subseteq S$, C is an ideal of R, Q.E.D.

(3.25) Proposition. Let K be a field and let $R = K[x^2, x^3]$ where x is an indeterminate. Let S be the integral closure of R. Then

(i.) $S = K[x]$.

(ii.) $C = (x^2, x^3)$.

(iii.) C is a maximal ideal of R.

Proof. (i.) First, $x \in K[x]$ is integral over R since x satisfies the polynomial $\mathbb{X}^2 - x^2 \in R[\mathbb{X}] = K[x^2, x^3][\mathbb{X}]$, where $\mathbb{X}$ is an indeterminate. Thus $x \in S$. Since the

set of integral elements over R forms a ring, $K[x] \subseteq S \subseteq K(x)$ where $K(x) = \{f(x)/g(x) \mid f,g \in K[x], g \neq 0\}$ is the quotient field of R. To see that $S \subseteq K[x]$, let $f(x)/g(x) \in S$. If $g(x) = g_1(x)g_2(x)$ then $g_1(x) \in K[x] \subseteq S$. So $g_1(x)(f(x)/(g_1(x)g_2(x))) = f(x)/g_2(x) \in S$. If $g_2(x)$ is reducible then we can continue the process in this same fashion until we have $f(x)$ over an irreducible poynomial. Thus, we can assume that $g(x)$ is irreducible in $K[x]$. Then there exist $a_i \in R$ such that

$$(f(x)/g(x))^n + a_1(f(x)/g(x))^{n-1} + \ldots + a_{n-1}(f(x)/g(x)) + a_n = 0.$$

$$f^n(x)/g^n(x) + a_1 f^{n-1}(x)/g^{n-1}(x) + \ldots + a_{n-1}f(x)/g(x) + a_n = 0.$$

$$g^n(x)\,(f^n(x)/g^n(x) + a_1 f^{n-1}(x)/g^{n-1}(x) + \ldots + a_{n-1}f(x)/g(x) + a_n) = 0.$$

$$f^n(x) + a_1 f^{n-1}(x)g(x) + \ldots + a_{n-1}f(x)g^{n-1}(x) + a_n g^n(x) = 0.$$

$$f^n(x) = -(a_1 f^{n-1}(x)g(x) + \ldots + a_{n-1}g^{n-1}f(x) + a_n g^n(x)).$$

$$f^n(x) = -(a_1 f^{n-1}(x) + \ldots + a_{n-1}g^{n-2}(x)f(x) + a_n g^{n-1}(x))(g(x)).$$

Since $g(x)$ is irreducible, $g(x) \mid f(x)$ thus $f(x)/g(x)$ is an element of $K[x]$.

(ii.) To see that $C = (x^2, x^3)$ let $f(x) = a_o + a_1x + \ldots + a_nx^n \in C$. By definition $f(x)S \subseteq R$. So $(a_o + a_1x + \ldots + a_nx^n)S \subseteq R = K[x^2, x^3]$. Since $1 \in S$, then $((a_o + a_1x + \ldots + a_nx^n) \cdot 1) \in R$ which implies that $a_o + a_1x + \ldots + a_nx^n \in R$. Thus $a_1 = 0$ since no element of R has an x term. Similarly, $f(x)x \in R$ implies that $a_o = 0$. So $f(x) \in (x^2, x^3)$. Therefore $C \subseteq (x^2, x^3)$.

For the other containment, let $f(x) = a_o + a_1x + \ldots + a_nx^n$ be a polynomial in S. Then x^2f has no x term since $x^2f(x) = x^2(a_o + a_1x + \ldots + a_nx^n) = a_ox^2 + a_1x^3 + \ldots + a_nx^{n+2}$. Further, $x^3f(x)$ has no x term either since $x^3f(x) = x^3(a_o + a_1x + \ldots + a_nx^n) = a_ox^3 + a_1x^4 + \ldots + a_nx^{n+3}$. Thus we have that $C \supseteq (x^2, x^3)$. So we have identified the integral closure and conductor of $K[x^2, x^3]$.

(iii.) To see that C is a maximal ideal of R we define $f: R \rightarrow K$ by $f(a_o + a_2x^2 + a_3x^3 + \ldots + a_nx^n) = a_o$. Let x and y be elements of R such that $x = a_o + a_2x^2 + a_3x^3 + \ldots + a_nx^n$ and $y = b_o + b_2x^2 + b_3x^3 + \ldots + b_nx^n$, for a_i and b_i elements of K. We verify that f is a ring homomorphism:

$$f(x + y) = f(a_o + b_o + (a_2 + b_2)x^2 + (a_3 + b_3)x^3 + \ldots + (a_n + b_n)x^n$$
$$= a_o + b_o$$
$$= f(x) + f(y).$$

$$f(xy) = f(a_ob_o + a_ob_2x^2 + a_ob_3x^3 + \ldots + a_2b_ox^2 + a_2b_2x^4 + a_2b_3x^5 + \ldots + a_nb_ox^n + a_nb_2x^{n+2} + a_nb_3x^{n+3} + \ldots + a_nb_nx^{2n}$$
$$= a_ob_o$$
$$= f(x)f(y).$$

Next we show that ker f = C. Let $t = a_o + a_2x^2 + a_3x^3 + \ldots + a_nx^n \in R$. Then $t \in \ker f$ if and only if $a_o = 0$ if and only if $t \in (x^2, x^3)$. We have that f induces an isomorphism of rings $R/C \cong K$ [8]. Since K is defined to be an arbitrary field we have that C is a maximal ideal [9], Q.E.D.

(3.26) Definition. If S is an extension ring of R and $I(\neq S)$ is an ideal of S, then the ideal $J = I \cap R$ is called the contraction of I to R.

(3.27) Definition. A discrete valuation ring, DVR, is a principal ideal domain that has exactly one nonzero prime ideal.

(3.28) Lemma. If R is a PID then R_M is a DVR whenever

M is a maximal ideal of R.

Proof. Let J be a nonzero prime ideal of R_M. If R is a PID then R_M is a PID. Thus dim R_M = 1 [10]. So $J = I_M$ where I is a nonzero prime ideal of R that is contained in M and $J \supset 0$ is a chain of prime ideals of maximum length. Therefore J is a maximal ideal. Since MR_M is the only maximal ideal of R_M, $J = MR_M$, so MR_M is the only prime ideal in R_M, Q.E.D.

The next lemma corresponds to Pettersson's Lemma 5 [P]. The proof of the lemma utilizes the Lying-over Theorem which states that if S is an integral extension ring of R and if P is a prime ideal of R, then there exists a prime ideal Q in S such that $Q \cap R = P$, i.e. Q lies over P. In particular, if M is a maximal ideal of R then M is also a prime ideal of R. Thus there exists a prime ideal N of S such that $M = N \cap R$.

We give the statement of the next lemma without proof. We note that the proof can be found in [P].

(3.29) Lemma. Let R be a one-dimensional Noetherian integral domain. Let S be the integral closure of R. Let C be the conductor of R in S. If M is a maximal ideal of R such that $M \nsupseteq C$, M is the contraction of the prime ideal N of S. Then N is a maximal ideal of S, R_M is a DVR, and $R_M = S_N$.

(3.30) Theorem. Let $R = K[x^2,x^3]$ where K is a field and let $C = (x^2,x^3)$ be the conductor of R. Let M be a maximal ideal of R such that $M \neq C$. Then M is invertible and strongly two-generated.

Proof. Let $S = K[x]$ be the integral closure of R (Proposition 3.25). Then M is the contraction of a maximal ideal N of S [11]. By Proposition 3.11, it suffices to show that MR_Q is a principal ideal for all maximal ideals Q of R. For $Q \neq M$ then there exists $s \in M-Q$ such that $1 = s/s \in MS_Q$. Thus $MS_Q = R_M = (1)$ and MR_Q is principal in this case.

Suppose $Q = M$. Let N be a maximal ideal of S such that $N \cap R = M$. S is a principal ideal domain so S_N is a principal ideal domain. By Lemma 3.29, $S_N = R_M$, so MR_Q is a principal ideal for all maximal ideals Q of R. Thus M is invertible (Proposition 3.11) and M is strongly two-generated (Proposition 3.13), Q.E.D.

Recall that the goal of this paper is to characterize strong two-generators in certain commutative domains. From this point on we will let $R = K[x^2,x^3]$ where K is an arbitrary field. Note that the quotient field of $K[x^2,x^3]$ is $K(x) = \{f(x)/g(x)$ such that $f,g \in K[x]$, $g \neq 0\}$ by Proposition 3.25.

(3.31) Lemma. Let $R = [x^2,x^3]$ for K an arbitrary field. Then the fractional ideal $(1,x)$ is invertible if and only if the ordinary ideal (x^2,x^3) is invertible.

Proof. Assume that (x^2,x^3) is invertible. Then $(x^2,x^3))(x^2,x^3)^{-1} = R$. We note that the elements of $(x^2,x^3)^{-1}$ are fractions from the quotient field of R. There exist elements $(f_1(x)/g_1(x))$, $(f_2(x)/g_2(x))$ in $(x^2,x^3)^{-1}$ such that $1 = x^2(f_1(x)/g_1(x)) + x^3(f_2(x)/g_2(x))$ $= 1(x^2f_1(x)/g_1(x)) + x(x^2f_2(x)/g_2(x))$. Both $x^2f_i/g_i \in (1,x)^{-1}$ since $(x^2f_i(x)/g_i(x))1 = (x^2f_i(x)/g_i(x))(x^2/x^2)$ $= (f_i(x)/g_i(x))(x^2) \in R$ and $(x^2f_i(x)/g_i(x))x =$ $(x^2f_i(x)/g_i(x))(x^3/x^2) = (f_i(x)/g_i(x))x^3 \in R$. Thus $1 \in (1,x)(1,x)^{-1} = R$.

Next we show that if $(1,x)$ is an invertible ideal of R then (x^2,x^3) is too. Assume that $(1,x)$ is an invertible ideal of R. Then $(1,x)(1,x)^{-1} = R$. Thus for $i = 1,2$, there exists $f_i(x)/g_i(x) \in (1,x)^{-1}$ such that $1 = 1(f_1(x)/g_1(x)) + x(f_2(x)/g_2(x))$. This implies that $1 = (x^2/x^2)(f_1(x)/g_1(x)) + (x^3/x^2)(f_2(x)/g_2(x))$ $= x^2f_1(x)/(x^2g_1(x)) + x^3f_2(x)/(x^2g_2(x))$. Both $f_1(x)/(x^2g_1(x))$ and $f_2(x)/(x^2g_2(x))$ are elements of $(x^2,x^3)^{-1}$ since $(f_i(x)/x^2g_i(x))x^2 = (f_i(x)/g_i(x))1 \in R$ and $(f_i(x)/x^2g_i(x))x^3 = (f_i(x)/g_i(x))x \in R$. So $1 \in (x^2,x^3)(x^2,x^3)^{-1}$. Thus $(1,x)$ is invertible if and

only if (x^2,x^3) is invertible, Q.E.D.

In Proposition 3.25 we showed that the integral closure of $R = K[x^2,x^3]$ is $S = K[x]$. From the Lying-over Theorem we have that if P is a prime ideal in R then there exists a prime ideal Q in S such that $Q \cap R = P$. Since K[x] is a one-dimensional Noetherian integral domain so is $K[x^2,x^3]$, [12].

(3.32) Theorem. Let $R = K[x^2,x^3]$ and $C = (x^2,x^3)$ be the conductor of R in S. Then C is the only non-invertible maximal ideal in R.

Proof. From Proposition 3.24 and Theorem 3.30 it suffices to show that C is non-invertible. We do this by showing that (1,x) is not invertible (Proposition 3.31). Assume $f(x)/g(x) \in (1,x)^{-1}$. Then $(f(x)/g(x))1$ is an element of R. Thus g(x) divides f(x), so $(1,x)^{-1}$ is a subset of K[x]. Let $f(x)/g(x) = h(x) \in (1,x)^{-1} \subseteq K[x]$. Then $h(x) = a_o + a_1x + \ldots + a_nx^n$ such that a_i's $\in K$. Since $1(h(x)) \in R$ then $1(a_o + a_1x + \ldots + a_nx^n) \in R$. Also, $x(h(x)) \in R$ so $x(a_o + a_1x + \ldots + a_nx^n) \in R$. There can be no x term in R so both a_o and a_1 equal 0. Thus $h(x) = a_2x^2 + \ldots + a_nx^n \in (x^2,x^3)$.

So $(1,x)(1,x)^{-1} \subseteq (1,x)C \subseteq C \neq R$ and (1,x) is not invertible nor is (x^2,x^3) by Lemma 3.31, Q.E.D.

Our final theorem characterizes strong

two-generators in $K[x^2,x^3]$ for K an arbitrary field.

(3.33) Theorem. Let $R = K[x^2,x^3]$ for K an arbitrary field. Let $f = a_o + a_2x^2 + a_3x^3 + \ldots + a_nx^n$ be a nonzero polynomial in $K[x^2,x^3]$ and let $C = (x^2,x^3)$ be the conductor of R in S. Then the following are equivalent:

(1) f is a strong two-generator.

(2) $f \notin C^2$.

(3) $a_o \neq 0$ or if $a_o = 0$ then $x^2 \mid f$ but $x^4 \nmid f$.

Proof.

(1) if and only if (2).

From Theorem 3.32, C is the only non-invertible ideal in R. By Theorem 3.18, f is a strong two-generator in R if and only if f is not an element of C^2.

(2) implies (3).

We first note that $C^2 = (x^4,x^5,x^6)$. Assume $f \notin C^2$ and $a_o = 0$. Then $f = a_2x^2 + a_3x^3 + \ldots + a_nx^n$, where a_2 and a_3 are not both equal to 0. Since one of $a_i \neq 0$ for $i = 2,3$, $x^2 \mid f$ but $x^4 \nmid f$.

(3) implies (2)

If $a_o = 0$ then $f = a_o + a_2x^2 + \ldots a_nx^n \in C^2 = (x^4,x^5,x^6)$. If $a_o = 0$ and $x^4 \nmid f$ then a_2 or $a_3 \neq 0$. Thus $f = a_2x^2 + \ldots + a_nx^n \notin C^2 = (x^4,x^5,x^6)$, Q.E.D.

We have completed the objective of this paper.

We conclude with an example of a polynomial which is a strong two-generator and another that is not.

(3.34) Example. Choose $f = 1 + x^2$. Then f is a strong two-generator since $a_o = 1$ (Theorem 3.33(3)).

(3.35) Example. Let $g = x^4 + x^5$. Then $g = x^4(1 + x)$. So $a_o = 0$ and $x^4 \mid g$, so g is not a strong two-generator.

APPENDIX

1. [A-M, Theorem 4.5, pg52] Let I be a decomposable ideal and let $I = \bigcap_{i=1}^{n} Q_i$ be a minimal primary decomposition of I. Let $P_i = \text{rad } Q_i$ for $i = 1,\ldots,n$. Then the P_i are precisely the prime ideals which occur in the set of ideals $\text{rad}(I:x)$, $x \in I$, and hence are independent of the particular decomposition of I.

2. [A-M, Theorem 8.5, pg90] A ring A is Artin if and only if A is Noetherian and dim A = 0.

3. [A-M, Proposition 6.6, pg76] If R is Noetherian ring and (a) is an ideal of R then R/(a) is a Noetherian ring.

4. [H, Theorem 43, pg143] S, R, and $S^{-1}R$ are as defined in the paper. If R is a nonzero ring with no zero divisors and $0 \notin S$, then $S^{-1}R$ is an integral domain.

5. [H, Theorem 47, pg145] R and S are the same as in the paper. If I is an ideal of R then $S^{-1}I$ is an ideal in $S^{-1}R$.

6. [A-M, Lemma 4.4, pg51] If M_i is an associated prime ideal of the primary ideal Q_i and $x \in R$, then (i) if $x \in Q_i$ then $(Q_i:x) = (1)$, (ii) if $x \notin Q_i$ then $\text{rad } (Q_i:x) = M_i$, and (iii) if $x \notin M_i$ then $(Q_i:x) = Q_i$.

7. [A-M, Corollary 3.4iii, pg39] If (a) is a submodule of an R-module then the $S^{-1}R$ modules $S^{-1}(I/(a))$ and $(S^{-1}I)/(S^{-1}(a))$ are isomorphic.

8. [H, Corollary 2.10: First Isomorphism Theorem, pg126] If f: R$\rightarrow$K is a homomorphism of rings then f induces an isomorphism of rings R/ker f $\cong$ K.

9. [A-M, pg3] C is an ideal of a ring A. C is a maximal ideal if and only if A/C is a field.

10. [A-M, Dimension Theorem, pg121] For any Noetherian local ring R with M its maximal ideal, the following integers are equivalent: (i) the maximum length of chains of prime ideals in R, and (iii) the least number of generators of an M-primary ideal of R. Note: If M = rad Q then Q is said to be M-primary.

11. [A-M, Corollary 5.8, pg61] Let R$\subseteq$S be rings, S integral over R; let N be a prime ideal of S and let M = N$\cap$R. Then N is maximal if and only if M is maximal.

12. [K, Theorem 48, pg32] Let R = $K[x^2,x^3]$ and S = K[x]. Then R$\subset$S and S is integral over R. Thus dimension of S equals the dimension of R.

BIBLIOGRAPHY

[A-M] Atiyah, M.F. and I.G. MacDonald, Introduction to Commutative Algebra. Reading, Mass.: Addison-Wesley Publishing Company, Inc., 1969.

[C] Chapman, Scott, Characterizing Strong Two-generators in $K[X^2,X^3]$. Houston Journal of Mathematics, Volume 16, No. 2, (1990)217-229.

[F] Fraleigh, John B., A First Course In Abstract Algebra, 5th ed. Menlo Park, CA.: Addison-Wesley Publishing Company, Inc., 1994.

[H] Hungerford, Thomas W., Algebra. New York, N.Y.: Springer-Verlag, 1974.

[K] Kaplansky, I., Commutative Rings. Boston, Mass.: Allyn and Bacon, 1970.

[L] Lambek, Joachim, Lectures On Rings and Modules. New York, N.Y.: Chelsea Publishing Company, 1986.

[P] Pettersson, Kerstin, Strong n-Generators In Some One-Dimensional Domains. Communications In Algebra, 22(8), (1994)2941-2953.